



Law Offices of Bennet & Bennet, PLLC

Maryland

4350 East West Highway, Suite 201
Bethesda, Maryland 20814
Tel: (202) 371-1500
Fax: (202) 371-1558

District of Columbia

10 G Street NE, Suite 710
Washington, DC, 20002

Caressa D. Bennet

Michael R. Bennet

Gregory W. Whiteaker

Marjorie G. Spivak*

Donald L. Herman, Jr. +

Kenneth C. Johnson‡

Howard S. Shapiro†

Daryl A. Zakov^

Robert A. Silverman

Of Counsel

Andrew Brown*

*Admitted in DC & PA Only

+Admitted in DC & AL Only

†Admitted in DC, VA & FL Only

‡Admitted in DC & VA Only

^Admitted in WA Only

↯Admitted in DC & ME Only

September 19, 2008

Via ECFS

Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
445 12th Street, SW
Washington, DC 20554

Re: CPNI Certification and Accompanying Statement
EB Docket No. 06-36

Dear Ms. Dortch:

OTZ Telecommunications, Inc., by its attorneys and pursuant to Section 64.2009(e) of the Commission's Rules, hereby submits its CPNI certification and accompanying statement.

Should you have any questions or need further information, please contact the undersigned.

Sincerely,

/s/

Michael R. Bennet

cc: Telecommunications Consumers Division, Enforcement Bureau
Best Copy and Printing, Inc.

Attachments

CPNI Compliance Certificate

I, Doug Neal, certify that I am an officer of OTZ Telecommunications, Inc. ("OTZ"). Pursuant to Section 64.2009(e) of the Rules and Regulations of the Federal Communications Commission, I hereby certify that I have personal knowledge that OTZ has established operating procedures that are adequate to ensure compliance with the FCC's CPNI rules.

Attached to this certification is an accompanying statement explaining how OTZ's procedures ensure that it is in compliance with the requirements set forth in Section 64.2001 *et seq.* of the FCC's rules.

OTZ has not taken any action against data brokers in the past year. OTZ has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed: Doug Neal

Date: 9-17-08

CPNI Compliance Accompanying Statement:

This accompanying statement explains how OTZ Telecommunications' operating procedures ensure that the company is in compliance with the rules governing CPNI as found in Subpart U – Customer Proprietary Network Information – Part 64 of Title 47 of the Code of Federal Regulations.

OTZ Telecommunications adheres to all CPNI rules as stated in section 64.2001 – 64.2011 concerning the proper use of our customer's CPNI. Specifically, our notice for use of CPNI approval process meets all requirements as listed in Section 64.2008. To further protect our customer's privacy, we have implemented all safeguards required in Section 64.2009. This includes:

- The implementation of a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI;
- The training of appropriate personnel as to when they are, and are not, authorized to use CPNI and the documentation of this training;
- The implementation of an express disciplinary process for CPNI violations up to and including termination;
- The maintenance of a record, for at least one year, of our own, and our affiliates' sales and marketing campaigns ;
- The establishment of a supervisory review process regarding carrier compliance with the federal CPNI rules for outbound marketing situations; and
- The establishment of annual certification by a corporate officer with personal knowledge of OTZ Telecommunications' policies and procedures to ensure compliance with the federal CPNI rules.
- The establishment of procedures for notification of the Commission of any instance where opt-out mechanisms, do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

OTZ Telecommunications is including its CPNI Manual, without the sample Forms, as further detailed explanation of how its procedures ensure that it is in compliance with the rules in Subpart U of Part 64, of Title 47 of the Code of Federal Regulations.



OTZ Telecommunications

CPNI

POLICIES & PROCEDURES

MANUAL

Approved by:

Chief Executive Officer

Date

Effective: _____

TABLE OF CONTENTS

<i>Definitions</i>	3
<i>Company Policy regarding CPNI</i>	6
<i>Marketing Programs</i>	7
<i>Release of Call Detail Information</i>	7
<i>Annual Certification</i>	9
<i>Notice of Unauthorized Disclosure of CPNI</i>	9
 <i>Safeguards by OTZ TELECOMMUNICATIONS</i>	12
 <i>Training of Employees</i>	14
 <i>Annual Review by Company Management</i>	15
 <i>Forms</i>	
<i>Form 1 – Employee Training Certification</i>	16
<i>Form 2 – Certification of CPNI Filing</i>	17
<i>Form 3 – Breach Notification – Law Enforcement</i>	18
<i>Form 4 – Breach Notification – Customer</i>	19
<i>Form 5 – Notification of Account Changes</i>	20
<i>Form 6 – Certification of Marketing Campaign Effort</i>	21
<i>Form 7-W – CPNI Customer Notification (with password)</i>	22
<i>Form 7-WO - CPNI Customer Notification (without password)</i>	25
<i>Form 8-W – Annual CPNI Notice (with password & opt out)</i>	28
<i>Form 8-WO – Annual CPNI Notice (without password)</i>	30
<i>Form 9 – Record of Customer Complaints Concerning the Unauthorized Release of CPNI</i>	31
<i>Form 10 – Notice of Failure of Opt-out Mechanism</i>	32

Definitions

This OTZ TELECOMMUNICATIONS CPNI policy manual relies on the following definitions:

- (1) **Account information.** “Account information” is information that is specifically connected to the customer’s service relationship with OTZ TELECOMMUNICATIONS, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill’s amount.
- (2) **Address of record.** An “address of record,” whether postal or electronic, is an address that the carrier has associated with the customer’s account for at least 30 days.
- (3) **Affiliate.** The term “affiliate” means a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another to own an equity interest (or the equivalent thereof) of more than 10 percent.
- (4) **Breach.** When a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.
- (5) **Call detail information.** Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.
- (6) **Communications-related services.** The term “communications-related services” means telecommunication services, information services typically provided by OTZ TELECOMMUNICATIONS and services related to the provision or maintenance of customer premises equipment.
- (7) **Customer.** A customer of OTZ TELECOMMUNICATIONS is a person or entity to which OTZ TELECOMMUNICATIONS is currently providing service.
- (8) **Customer premises equipment (CPE).** The term “customer premises equipment (CPE)” means equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications.
- (9) **Customer Proprietary Network Information.** The term “customer proprietary network information” means –
 - (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of OTZ TELECOMMUNICATIONS, and that is made available to OTZ TELECOMMUNICATIONS solely by virtue of the OTZ TELECOMMUNICATIONS-customer relationship; and
 - (B) information contained in the bill pertaining to telephone exchange service or telephone toll service received by a customer of OTZ TELECOMMUNICATIONS; except that such term does not include subscriber list information.

- (10) **Data broker.** A person or business that offers for sale CPNI obtained by pretexting.
- (11) **Data bureau.** A company that provides information technology services to telecommunications carriers, specifically billing services and customer record detail. Data bureaus typically have access to call detail CPNI (see Independent contractor).
- (12) **FCC.** The acronym “FCC” refers to the Federal Communications Commission.
- (13) **Independent contractor.** Any person or business that may provide services to telecommunications carriers. This includes, but is not limited to; joint venture partners and independent contractors for the purposes of marketing communications-related services to a customer; billing services; customer record detail; central office equipment vendors; engineering; and construction. Independent contractors typically have access to call detail and/or non-call detail CPNI.
- (14) **Information services typically provided by OTZ TELECOMMUNICATIONS.** The phrase “information services typically provided by OTZ TELECOMMUNICATIONS” means only those information services that are typically provided by OTZ TELECOMMUNICATIONS, such as Internet access or voice mail services. Such phrase “information services typically provided by OTZ TELECOMMUNICATIONS,” as used in this manual, shall not include retail consumer services provided using Internet website (such as travel reservation services or mortgage lending services), whether or not such services may other wise be considered to be information services.
- (15) **Joint venture partners** (short term alliances of telecommunications carriers) **and independent contractors** (see Independent contractors) **for the purposes of marketing communications-related services to a customer.** A specific subset of persons or businesses that provide marketing services to telecommunications carriers. Any marketing use of CPNI by this subset must have opt-in approval by the affected customers.
- (16) **Local exchange carrier (LEC).** The term “local exchange carrier (LEC)” means any person that is engaged in the provision of telephone exchange service or exchange access. Such term does not include a person insofar as such person is engaged in the provision of a commercial mobile service under section 332(c) of TA-96, except to the extent that the Commission finds that such service should be included in the definition of such term.
- (17) **Opt-in approval.** The term “opt-in approval” refers to a method for obtaining customer consent to use, disclose, or permit access to the customer’s CPNI. This approval method requires that OTZ TELECOMMUNICATIONS obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the OTZ TELECOMMUNICATIONS’s request consistent with the requirements.
- (18) **Opt-out approval.** The term “opt-out approval” refers to a method for obtaining customer consent to use, disclose, or permit access to the customer’s CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer’s CPNI if the customer has failed to object thereto within the

waiting period described after the customer is provided appropriate notification of OTZ TELECOMMUNICATIONS's request for opt-out consent consistent with the rules.

- (19) **Password.** The term “password” means a secret word or sequence of alpha and numeric characters which is used to limit access to a customer’s account to authorized individuals.
- (20) **Pretexting.** The term “pretexting” means the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer’s call detail or other private communications records.
- (21) **Readily available biographical information.** “Readily available biographical information” is information drawn from the customer’s life history and includes such things as the customer’s social security number, or the last four digits of that number; mother’s maiden name; home address; or date of birth.
- (22) **Subscriber list information (SLI).** The term “subscriber list information” means any information –
 - (A) identifying the listed names of subscribers of OTZ TELECOMMUNICATIONS and such subscribers’ telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and
 - (B) OTZ TELECOMMUNICATIONS or an affiliate has published, caused to be published, or accepted for publication in any directory format.
- (23) **OTZ TELECOMMUNICATIONS or carrier.** The terms “OTZ TELECOMMUNICATIONS Telecom,” “OTZ TELECOMMUNICATIONS,” or “carrier” shall have the same meaning.
- (24) **Telecommunications service.** The term “telecommunications service” means the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.
- (25) **Telephone number of record.** The telephone number associated with the underlying service, not the telephone number supplied as a customer’s “contact information.”
- (26) **Valid photo identification.** The term “valid photo identification” means an official identification document issued by a federal or state governmental agency that identifies the holder of the document that includes a photograph of sufficient clarity to positively identify the holder of the document.

Company Policy Regarding CPNI

OTZ TELECOMMUNICATIONS may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (*i.e.*, local, long distance, and CMRS (wireless)) to which the customer already subscribes from OTZ TELECOMMUNICATIONS, without customer approval.

OTZ TELECOMMUNICATIONS may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. OTZ TELECOMMUNICATIONS may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI to its agents and its affiliates that provide communications-related services for the purpose of marketing communications-related services to that customer. OTZ TELECOMMUNICATIONS may also permit such persons or entities to obtain access to such CPNI for such purposes.

Except for use and disclosure of CPNI that is permitted without customer approval or for marketing as described above, OTZ TELECOMMUNICATIONS may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval. Accordingly, OTZ TELECOMMUNICATIONS's personnel are trained in the appropriate use of CPNI for such purposes.

OTZ TELECOMMUNICATIONS will notify (Form 10) the FCC in writing within five days of any instance when its opt-out policies did not work properly, to such a degree that the customer's inability to opt-out is more than an anomaly.

In this effort, the Company must follow all applicable FCC rules as contained in Subpart U – Customer Proprietary Network Information – of Part 64 of Title 47 of the Code of Federal Regulations. Specific OTZ TELECOMMUNICATIONS procedures are as follows:

BUSINESS CUSTOMER EXEMPTION

If a business customer of OTZ TELECOMMUNICATIONS has in place a contract for service with OTZ TELECOMMUNICATIONS that specifies:

- (1) a dedicated OTZ TELECOMMUNICATIONS account representative as the primary contact,
- (2) who can be reached without going through a call center, and
- (3) OTZ TELECOMMUNICATIONS's protection of that business customer's CPNI,

then OTZ TELECOMMUNICATIONS's authentication policies and procedures do not apply to that business customer. Specifically, the customer does not need to provide a password or the correct response to a back up means of authentication prior to the dedicated account representative discussing call detail CPNI with that customer during a customer-initiated telephone contact.

In the event that the dedicated account representative is unavailable for a customer-initiated telephone contact, a primary and a secondary account representative have been established by

OTZ TELECOMMUNICATIONS Either one of these may discuss call detail CPNI with the business customer during the period of unavailability of the dedicated account representative.

ACCESS TO CPNI DATA

Access to CPNI data is limited to employees or entities with the requisite proper authorization as allowed by FCC rules. Any employees or entities with CPNI access must operate under policies that require nondisclosure of confidential information. Improper use or disclosure of CPNI by employees is subject to disciplinary action up to and including termination.

Marketing Programs

OTZ TELECOMMUNICATIONS occasionally uses CPNI to target its marketing campaigns. OTZ TELECOMMUNICATIONS may use either opt-out or opt-in (Form 8-W) approval in determining its target customers.

Contact the Chief Executive Officer if you are uncertain as to the type of information you can use in marketing services to customers.

CUSTOMER NOTICE AT INITIATION OF SERVICE

Customers are informed during the initiation of service with OTZ TELECOMMUNICATIONS that their CPNI data is not used for marketing purposes. Customers receive annual reminders (Form 8-W or Form 8-WO) of this CPNI policy.

CUSTOMER NOTICE

Adequate notice with respect to customer CPNI rights and OTZ TELECOMMUNICATIONS's duty to protect CPNI is provided in OTZ TELECOMMUNICATIONS's telephone directory. In addition, a CPNI notice is printed periodically on the customer's billing statement.

RECORD OF CUSTOMER COMPLAINTS CONCERNING THE UNAUTHORIZED RELEASE OF CPNI

All customer complaints concerning the unauthorized release of CPNI will be logged (Form 9) and retained for a period of five years. This information is summarized and included with OTZ TELECOMMUNICATIONS's annual certification to the FCC.

Release of Call Detail Information (Forms 7-W or 7-WO & 8-W or 8-WO)

CUSTOMER INITIATED TELEPHONE ACCOUNT ACCESS

Release of any CPNI information requested by the customer via a telephone call is prohibited except when:

- the requesting individual provides the password of record; or
- the information will be sent via mail USPS to the customer's address of record; or
- OTZ TELECOMMUNICATIONS will call the telephone number of record and disclose the call detail information.

If the customer has forgotten their password or does not have a password established, OTZ TELECOMMUNICATIONS can proceed with routine customer care procedures if the customer can provide all of the call detail information. OTZ TELECOMMUNICATIONS will not disclose any call detail other than the information the customer disclosed during that particular contact.

RETAIL LOCATION ACCOUNT ACCESS

Customers or their authorized contacts as allowed by the Telecommunications Act of 1996 – Section 222(c)(2) must have a valid, government issued photo identification, such as a driver's license, passport, or comparable ID to obtain CPNI information.

ON-LINE ACCOUNT ACCESS

OTZ TELECOMMUNICATIONS requires an on-line password to protect on-line access to CPNI. Passwords will be designed by the customer and will consist of alpha and numeric characters. On-line passwords are not required if the customer chooses to receive call detail information via either of the two methods above.

OTZ TELECOMMUNICATIONS will authenticate both new and existing customers seeking on-line access to their CPNI.

OTZ TELECOMMUNICATIONS can reinitialize existing passwords for on-line access but will NOT base on-line access on readily available biographical or account information. This procedure will relate to all customer information, not just call detail.

On-line access to CPNI will be blocked after four (4) unsuccessful attempts to log on.

NOTIFICATION OF ACCOUNT CHANGES

OTZ TELECOMMUNICATIONS will notify (Form 5) any customer immediately of any account changes including password, customer response to company designed back-up means of authentication, on-line account, address of record, and any other record that may be created or changed. This notification will be through a voicemail or by USPS mail to the address of record as it was prior to the change.

New customers are exempt from this notification at service initiation.

PROCEDURES TO PROTECT AGAINST PRETEXTING

Pretexting is the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications record. The Company has employed the above procedures and safeguards in order to achieve reasonable measures designed to discover and protect against pretexting.

Annual Certification

OTZ TELECOMMUNICATIONS will certify annually (Form 2) compliance to the CPNI rules. This certification will be filed with the FCC and will be made publicly available by request.

OTZ TELECOMMUNICATIONS's annual certification will be signed by an officer as an agent of OTZ TELECOMMUNICATIONS, stating that he/she has personal knowledge the company has established operating procedures that are adequate to comply with the FCC CPNI rules.

In addition to the annual certification, OTZ TELECOMMUNICATIONS will provide an accompanying statement explaining how the company's procedures ensure the company is or is not in compliance with the FCC's CPNI rules. In the explanation, OTZ TELECOMMUNICATIONS will include:

- the training employees receive to protect CPNI.
- the disciplinary process applicable to improper disclosure of CPNI.
- the process used to ensure all requests to opt-in or opt-out are recorded, and follow-up methods used.
- other measures relevant to demonstrate compliance with the FCC's CPNI rules.

Notice of Unauthorized Disclosure of CPNI

OTZ TELECOMMUNICATIONS is required by FCC rules to notify law enforcement of any CPNI breaches no later than seven (7) days after a reasonable determination of a breach has occurred. OTZ TELECOMMUNICATIONS will send an electronic notification through the central reporting facility to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). This notification will include a description of the CPNI that was disclosed, how the breach was discovered, an analysis of the sensitivity of the breached CPNI, and any corrective measures taken to prevent recurrence of such breach.

Responsibility to notify USSS and FBI has been assigned to the Chief Executive Officer.

NOTIFICATION OF CPNI SECURITY BREACHES

- (1) *Notification of law enforcement agencies* (Form 3). OTZ TELECOMMUNICATIONS will notify law enforcement of a breach of its customers' CPNI as stated in this section of OTZ TELECOMMUNICATIONS's CPNI manual. OTZ TELECOMMUNICATIONS will not notify any of its customers or disclose the breach publicly, whether voluntarily or under

state or local law or these rules, until it has completed the process of notifying law enforcement as required and spelled out below.

- (2) *Limitations.* As soon as practicable, but in no event later than seven (7) business day, after reasonable determination of the breach, OTZ TELECOMMUNICATIONS shall electronically notify the **United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI)** through a central reporting facility. This will be done through the FCC's link to the reporting facility at <http://www.fcc.gov/eb/cpni>.
 - a) Notwithstanding any state law to the contrary, OTZ TELECOMMUNICATIONS shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as in the following two parts of this section.
 - b) If OTZ TELECOMMUNICATIONS believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under the above paragraph of this section, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. OTZ TELECOMMUNICATIONS shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.
 - c) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct OTZ TELECOMMUNICATIONS not to disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify OTZ TELECOMMUNICATIONS when it appears the public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to OTZ TELECOMMUNICATIONS, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writing shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.
- (3) *Customer Notification (Form 4).* After OTZ TELECOMMUNICATIONS has completed the process of notifying law enforcement as listed above, it shall notify its customers of a breach of those customers' CPNI.
- (4) *Recordkeeping.* OTZ TELECOMMUNICATIONS will maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI as defined in the above section of this manual, and all notifications made to customers. This record must include, if available:
 - a) Dates of discovery and notification.
 - b) A detailed description of the CPNI that was the subject of the breach.
 - c) The circumstances of the breach.

d) OTZ TELECOMMUNICATIONS will retain the record for a minimum of 2 years.

- (5) *Supersede.* This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

SAFEGUARDS BY OTZ TELECOMMUNICATIONS

CUSTOMER RECORDS

Customer service records will clearly establish customer CPNI approval. Record of this approval will be kept for a minimum of one year. The record is designed by OTZ TELECOMMUNICATIONS's service bureau which is MACC.

All personnel of OTZ TELECOMMUNICATIONS will be trained annually or upon commencement of employment regarding CPNI policies. These policies include when the employee is authorized to use and when they are NOT authorized to use CPNI. Any infractions of OTZ TELECOMMUNICATIONS's CPNI policies will be reported to the Chief Executive Officer and a record will be made of the infraction(s) and the disciplinary steps taken.

OTZ requires that all employees maintain strict confidentiality of customer information, and must refrain from discussing such information in the presence of other customers.

All Customer Service Representatives have access to privacy when discussing a customer's services and/or billing information, and must discuss such issues of confidential nature in the privacy of their offices.

In the event that confidentiality of a customer's information has been violated, depending upon the severity, the employee will receive disciplinary action up to termination.

All employees are required to sign a Non-Disclosure Agreement as a condition of employment. Employees, who disclose business information without prior approval from management, will be subject to disciplinary action up to termination, and legal action will be taken as necessary

INTERFACE WITH CALEA COMPLIANCE

In order to comply with certain Communications Assistance for Law Enforcement Agencies (CALEA) rules, OTZ TELECOMMUNICATIONS has engaged the services of a trusted third party provider. This third party provider is involved in the event of a request for certain types of surveillance activities by Law Enforcement Agencies (LEAs).

OTZ TELECOMMUNICATIONS has added the following addendum to its third party provider CALEA contract:

"Whereas OTZ TELECOMMUNICATIONS is required by law and its company policies to protect the privacy and security of the information regarding its customers,

To the extent that [Name of Third Party Provider], in rendering services for OTZ TELECOMMUNICATIONS receives customer proprietary network information, as that term is defined under 47 U.S.C. Section 222 and interpreted by the FCC ("CPNI"), [Name of Third Party Provider] shall maintain the confidentiality of such CPNI according to the policies and

procedures implemented by OTZ TELECOMMUNICATIONS. [Name of Third Party Provider] shall promptly delete from its records any CPNI that is received by [Name of Third Party Provider] which is not delivered to an LEA pursuant to a lawfully authorized intercept request.”
[Inset name, if desired (Intelleg, NeuStar, etc).]

INTERFACE WITH CONTRACTORS

OTZ TELECOMMUNICATIONS has occasion to utilize contractors for specific projects needed to conduct its business. OTZ TELECOMMUNICATIONS requires all its contractors to include the following language in all agreements with OTZ TELECOMMUNICATIONS:

“Whereas OTZ TELECOMMUNICATIONS is required by law and its company policies to protect the privacy and security of the information regarding its customers,

To the extent that [Name of Contractor], in rendering services for OTZ TELECOMMUNICATIONS receives customer proprietary network information, as that term is defined under 47 U.S.C. Section 222 and interpreted by the FCC (“CPNI”), [Name of Contractor] shall maintain the confidentiality of such CPNI according to the policies and procedures implemented by OTZ TELECOMMUNICATIONS. [Name of Contractor] shall promptly delete from its records any CPNI that is received by [Name of Contractor] in its engagement with OTZ TELECOMMUNICATIONS”

TRAINING OF EMPLOYEES

EMPLOYEE TRAINING

The company provides training to employees on the proper use and disclosure of CPNI. The company also provides written documentation of CPNI policy.

Included as a part of the employee training is the need to communicate to company employees that the customer is provided the opportunity to restrict company or affiliate use of CPNI data. The customer decision regarding OTZ TELECOMMUNICATIONS use of CPNI use will not affect OTZ TELECOMMUNICATIONS's provision of any current customer services.

OTZ TELECOMMUNICATIONS specific CPNI training will be provided annually and with each newly hired employee. Documentation of training (Form 1) will be kept on file for a period of at least five years.

ANNUAL REVIEW BY COMPANY MANAGEMENT

OTZ TELECOMMUNICATIONS treats customer privacy as a serious issue. OTZ TELECOMMUNICATIONS is proud of its long history of reliable, trustworthy service and is vigilant in the steps that will be taken to ensure customer privacy. Accordingly, OTZ TELECOMMUNICATIONS policy requires this CPNI Policy Manual to be reviewed on an annual basis. This review is conducted at a time set by the Chief Executive Officer each calendar year.

The Chief Executive Officer's annual review will include, but may not be limited to a review with GVNW Consulting, Inc. and a review with the Board of Directors.

Employee Training Certification - CPNI

I, undersigned, hereby acknowledge receiving and reviewing OTZ TELECOMMUNICATIONS's CPNI Manual. I have completed the training coordinated by OTZ TELECOMMUNICATIONS's CPNI Compliance Officer. I further understand my responsibilities to protect CPNI and the disciplinary procedures established by OTZ TELECOMMUNICATIONS concerning CPNI.

Name: _____

Position: _____

Date CPNI Manual Received: _____

Date CPNI Training: _____

Signature

Date

Witnessed by the CPNI Compliance Officer

Print Name

Signature

Date

Certification of CPNI Filing
[Section 64.2009(e) of FCC Rules]

I hereby certify that I am an Officer of OTZ TELECOMMUNICATIONS

I have personal knowledge that OTZ TELECOMMUNICATIONS established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information Rules and requirements in Part 64 Subpart U of the Federal Communications Commission's Rules. The attached Statement of CPNI Compliance explains how OTZ TELECOMMUNICATIONS's operating procedures ensure that it is in compliance with the applicable rules.

I am making this certification for the year _____.

Signature

Printed Name

Office Held

Date

Breach Notification – Law Enforcement

This notice has been generated to comply with Part 64 Subpart U of the Federal Communications Commission's Rules (47 C.F.R. §64.2011) which requires telecommunications carriers to notify the Federal Bureau of Investigation (FBI) and the United States Secret Service (USSS) when a breach to Customer Proprietary Network Information (CPNI) has been detected.

This message has been submitted to the FBI and the USSS via the FCC link - <http://www.fcc.gov/eb/cpni>

A description of the breach follows:

Customer Name on Account: _____

Phone Number: _____

Breach Performed By: _____

Description of Breach: _____

Sensitivity Analysis: _____

Corrective Measures: _____

Date Submitted: _____ (Must be reported within 7 days of breach)

Please contact Compliance Officer of OTZ TELECOMMUNICATIONS to provide instructions and/or gather more information regarding this breach of CPNI.

Signature

Date

Printed Name

Breach Notification - Customer

[Date]

[Customer Name]

[Address of Record]

[City, State Zip]

OTZ TELECOMMUNICATIONS respects your privacy and observes the privacy rules established by the Federal Communications Commission and the Regulatory Commission of Alaska.

This notice is being sent to you because a breach of your account information has occurred. In compliance with Part 64 Subpart U of the Federal Communications Commission's Rules, OTZ TELECOMMUNICATIONS was required to notify the Federal Bureau of Investigation and the United States Secret Service of the breach. Please see a summary of the breach information below:

Phone Number:_____ Date of Breach:_____

Description of Breach:_____

Date Submitted to Law Enforcement:_____

Please call our office to receive further information. We appreciate your business and strive to protect your information.

Sincerely,

Chief Executive Officer

Notification of Account Changes

[Date]

[Customer Name]

[Address of Record]

[City, State Zip]

OTZ TELECOMMUNICATIONS respects your privacy and observes the privacy rules established by the Federal Communications Commission and the Regulatory Commission of Alaska.

This notice is being sent to you because of changes made to your account. Current Federal Communications Commission rules require that we notify you of certain situations.

Please see the summary below that describes the reason for this notice. Should you have any questions, please do not hesitate to contact us.

Phone Number: _____

Name(s) on Account: _____

Recent changes or account activity:

- ☐ New password was created.
- ☐ Password has been changed.
- ☐ Address of record was changed.
- ☐ Email of record was changed.
- ☐ Back-up questions were used to re-issue a lost or forgotten password.

Account activity was recorded on [Date]. Thank you for your business with OTZ TELECOMMUNICATIONS.

Sincerely,

Chief Executive Officer

Certification of Marketing Campaign Effort

The attached marketing documents have been approved and are found to not violate Customer Proprietary Network Information (CPNI) rules established in Part 64 Subpart U of the Federal Communications Commission's Rules and OTZ TELECOMMUNICATIONS's CPNI Manual.

This certification is made by CPNI Compliance Officer for OTZ TELECOMMUNICATIONS

Signature

Printed Name

Date

Initial CPNI Customer Notification (With Password)

[Date]

To our Valued Customers,

Under federal law, you have the right to confidentiality of information regarding the telecommunication services to which you subscribe and OTZ TELECOMMUNICATIONS Telecom has the duty to protect that confidentiality. This confidential information includes such things as, specific services you purchase, the number of services purchased, who your provider is for a service, call detail records, and charges related to the services purchased. This information is referred to as Customer Proprietary Network Information (CPNI).

Due to the sensitive nature of CPNI, on April 2, 2007, the Federal Communications Commission (FCC) released new rules pertaining to the security of CPNI with special emphasis on call detail CPNI. Call detail CPNI refers to any and all information pertaining to the transmission of specific telephone calls such as telephone number called, telephone number calling, time, date, charges, location and duration of the telephone call.

Among the new rules is the option for you to establish a password with OTZ TELECOMMUNICATIONS and provide that password during a telephone call from you before we are authorized to disclose or discuss call detail records. For your protection, this password cannot derive from readily available biographical information such as your social security number, mother's maiden name, home address, or date of birth.

If you happen to lose or forget your password, OTZ TELECOMMUNICATIONS has implemented a back-up authentication method. We will ask that you provide us with a secret question. This secret question should prompt you for a response that will allow us to provide you with your password. Again, the secret question cannot derive from biographical information. As an example your secret question might be; what is the color of my eyes? or, what is my dogs' name? In which case, your back-up answers may be "Green" or "Gizmo" respectively.

If you choose not to establish a password and/or secret question, below are alternatives which can be used in order for us to discuss or provide you call detail information.

- OTZ TELECOMMUNICATIONS may discuss only the call detail information you provide such as called number, when it was called, the duration of the call, and, if applicable, the amount charged for the call.
- OTZ TELECOMMUNICATIONS can send the call detail information to the address of record that we have on file for you.
- OTZ TELECOMMUNICATIONS can call you back at the telephone number of record from which your service is derived.

- OTZ TELECOMMUNICATIONS may disclose call detail CPNI to you at our business office with a valid photo ID matching the name listed on the account. Note that we are only authorized to disclose call detail CPNI to the individual(s) listed on the account with a valid photo ID.

This password protection will become effective on December 8, 2007 so we strongly encourage you to establish your password and back-up secret question by completing the enclosed form and returning it to the address provided.

The new CPNI rules also require we notify you immediately if your password, your response to a backup means of authorization for lost or forgotten passwords, or address of record is created or changed. The means of notification may be by way of a telephone call from us to your telephone number of record, or by mail to the address of record as it was prior to the change.

Please feel free to contact OTZ TELECOMMUNICATIONS's local business office at (907) 442 - 3114 with any questions or concerns.

Sincerely,

Community Outreach Coordinator

Establishment of Account Password

So that OTZ TELECOMMUNICATIONS employees are free to discuss and/or provide call detail information to me during a call that I initiate to your business office, please establish the following password for my account.

Password: _____

Should I forget or lose my password please use the following question to authenticate my password.

Secret Question: _____

Answer: _____

Primary Customer Name: _____

Secondary Customer Name: _____

Additional Authorized Contacts: _____

Telephone Number: _____

Account Number: _____

Authorized Signature: _____

Date: _____ / _____ / _____

Please return completed form to:

OTZ TELECOMMUNICATIONS
PO Box 324
Kotzebue, AK 99752-0324

Contact telephone number for questions – (907) 442 -3114

Initial CPNI Customer Notification (No Password)

Date

To our Valued Customers;

Under federal law, you have the right to confidentiality of information regarding the telecommunication services to which you subscribe and OTZ TELECOMMUNICATIONS has the duty to protect that confidentiality. This confidential information includes such things as, specific services you purchase, the number of services purchased, who your provider is for a service, call detail records, and charges related to services purchased. This information is referred to as Customer Proprietary Network Information (CPNI).

Due to the sensitive nature of CPNI, on April 2, 2007, the Federal Communications Commission (FCC) released new rules pertaining to the security of CPNI with special emphasis on call detail CPNI. Call detail CPNI refers to any and all information pertaining to the transmission of specific telephone calls such as telephone number called, telephone number calling, time, date, charges, location and duration of the telephone call.

In compliance with FCC rules and to protect your call detail information to the best of our ability, OTZ TELECOMMUNICATIONS has opted to no longer disclose or discuss call detail information during a customer initiated telephone call unless the customer can provide the specific call detail information in question. The call detail information would include such things as the called number, date and time of the call and if applicable, the amount charged for the call. Effective December 8, 2007, the methods below will be the only way in which OTZ TELECOMMUNICATIONS may disclose or discuss your call detail records with you.

- OTZ TELECOMMUNICATIONS may discuss only the call detail CPNI you provide such as called number, when it was called, the duration of the call, and, if applicable, the amount charged for the call.
- OTZ TELECOMMUNICATIONS can call you back at the telephone number of record from which your service is derived.
- OTZ TELECOMMUNICATIONS can send the call detail information to the address of record that we have on file for you.
- OTZ TELECOMMUNICATIONS may disclose call detail CPNI to you at our business office with a valid photo ID matching the name listed on the account. Note that we are only authorized to disclose call detail CPNI to the individual(s) listed on the account with a valid photo ID.

The new CPNI rules also require we notify you immediately if address of record is created or changed. The means of notification may be by way of a telephone call from us to your telephone number of record, or by mail to the address of record as it was prior to the change.

Please feel free to contact OTZ TELECOMMUNICATIONS's local business office at (907) 442 - 3114 with any questions or concerns.

Sincerely,

Community Outreach Coordinator

Annual CPNI Notice

[Date]

To our Valued Customers;

OTZ TELECOMMUNICATIONS respects the privacy of our customers and our employees do everything possible to protect information that may be found in your account records. The Federal Communications Commission developed new rules in 2007 that require certain steps be taken to protect Customer Proprietary Network Information (CPNI).

CPNI rules require that every customer is given the opportunity to create a password. Any person who knows the password can then be given requested account information during a telephone call they initiate. If you choose not to establish a password, the account information is available in one of three ways:

- 1) we may call the telephone number of record and provide the account information;
- 2) we may mail the information to the address of record; or
- 3) we may provide the information at our office if we are presented with valid photo identification and the individual so identified is on the account.

We encourage you to establish a password and share it only with the persons you trust to have access to your account. This will allow for easier retrieval of your account information.

Enclosed is additional information regarding CPNI and how it is used in marketing campaigns. If you *elect not to (choose to)* receive targeted marketing, please fill out the form and return it to our office.

We do not anticipate that these new rules will interfere with quality customer service. If you wish to receive additional information regarding CPNI rules and how they are implemented in OTZ TELECOMMUNICATIONS, please call or stop by our office.

Sincerely,

Community Outreach Coordinator

OTZ TELECOMMUNICATIONS use of Customer Proprietary Network Information for Marketing

OTZ TELECOMMUNICATIONS respects your privacy and observes the privacy rules established by the Federal Communications Commission (FCC) and the [State] Public Utility Commission. Under federal law, you have the right to confidentiality of information regarding the telecommunication services to which you subscribe and OTZ TELECOMMUNICATIONS has the duty to protect that confidentiality. This confidential information includes such things as, specific services you purchase, the number of services purchased, who your provider is for a service, call detail records, and charges related to services purchased. This information is referred to as Customer Proprietary Network Information (CPNI).

OTZ TELECOMMUNICATIONS will never sell your account information or provide details of your telephone calls to other parties, unless required by law enforcement.

OTZ TELECOMMUNICATIONS is authorized by the FCC to market, without approval, services to our subscribers within the categories of service that are provided to those customers. Specifically, those services are local, long distance, and wireless. OTZ TELECOMMUNICATIONS provides local service, our affiliate [Affiliate I] provides long distance service, and our affiliate [Affiliate II] provides wireless service. From time to time we may market additional features within the service(s) already subscribed to from us or our affiliates.

From time to time we may notify you of additional products and services from outside the existing business relationship we have with you. OTZ TELECOMMUNICATIONS is permitted to market to our customers service offerings that do not rely upon Customer Proprietary Network Information (CPNI) (i.e. mass mailings). However, when this marketing is based on CPNI, you have the right to be excluded from these marketing campaigns.

If you choose to accept CPNI based marketing information, you need do nothing. However, if you prefer to be excluded from these marketing efforts, please complete, sign, and return the attached form. We will exclude you from any targeted marketing.

OR

If you choose to accept CPNI based marketing information, please complete, sign, and return the attached form. However, if you prefer to be excluded from these marketing efforts, you need do nothing. We will exclude you from any targeted marketing.

Your service from OTZ TELECOMMUNICATIONS will not be affected by this decision.

If you have any questions, please don't hesitate to call our office at (907) 442 - 3114 or stop in and we will be happy to discuss any concerns you might have.

Community Outreach Coordinator

Opt-out

I have read this notice and prefer to opt-out of OTZ TELECOMMUNICATIONS marketing of products and services outside of my existing scope of services.

This decision is effective 33 days following the date of this correspondence from OTZ TELECOMMUNICATIONS (30 days from the third day following this mailing) and remains in effect until changed by me.

Name: _____

Billing Address: _____

City / State / Zip: _____

Telephone Number: _____

Signature: _____

Date: _____ / _____ / _____

Opt-in

I have read this notice and choose to opt-in to OTZ TELECOMMUNICATIONS marketing of products and services outside of my existing scope of services.

This decision is in effect immediately upon receipt of this approval by OTZ TELECOMMUNICATIONS and remains in effect until changed by me.

Name: _____

Billing Address: _____

City / State / Zip: _____

Telephone Number: _____

Signature: _____

Date: _____ / _____ / _____

Annual CPNI Notice

Date

To our Valued Customers;

OTZ TELECOMMUNICATIONS respects the privacy of our customers and our employees do everything possible to protect information that may be found in your account records. The Federal Communications Commission developed new rules in 2007 that require certain steps be taken to protect Customer Proprietary Network Information (CPNI).

If requested, OTZ TELECOMMUNICATIONS will provide account information to our customers in one of the following ways:

- 1) we will verify the password you provided to us when you call in with questions about your CPNI.
- 2) we may call the telephone number of record and provide the account information;
- 3) we may mail the information to the address of record; or
- 4) we may provide the information at our office if we are presented with valid photo identification and the individual so identified is on the account.

We do not anticipate that these new rules will interfere with quality customer service. If you wish to receive additional information regarding CPNI rules and how they are implemented in OTZ TELECOMMUNICATIONS, please call or stop by our office.

Sincerely,

Community Outreach Coordinator

OTZ TELECOMMUNICATIONS

Record of Customer Complaints Concerning the Unauthorized Release of CPNI

Month	Year		
Name		Number	Address
Nature of Complaint			
Name		Number	Address
Nature of Complaint			
Name		Number	Address
Nature of Complaint			
Name		Number	Address
Nature of Complaint			
Name		Number	Address
Nature of Complaint			
Name		Number	Address
Nature of Complaint			
Name		Number	Address
Nature of Complaint			
Name		Number	Address
Nature of Complaint			

Retain for 5 years

Notification of Failure of Opt-out Mechanism

[Date]

Federal Communications Commission
Enforcement Bureau
Telecommunications Consumers Division
445 12th Street SW
Washington, DC 20554

re: Failure of Opt-out Mechanism

OTZ TELECOMMUNICATIONS Telecom experienced a failure of its opt-out mechanism for # customer(s). This failure was discovered on [date].

OTZ TELECOMMUNICATIONS offers its customers the opportunity to opt-out of targeted marketing through an annual mailing. The affected customers

_____.

OTZ TELECOMMUNICATIONS proposes to remedy the situation by

_____.

The Regulatory Commission of Alaska is receiving a copy of this correspondence. To date the RCA has not taken any action on this matter.

Attached is a copy of the notice provided to the affected customers.

For further information regarding this failure of OTZ TELECOMMUNICATIONS's opt-out mechanism, please contact me at (907) 442 - 3314.

Sincerely,

Chief Executive Officer

attachment
copy: Regulatory Commission of Alaska

[Date]

Customer Name
Customer Address
City, ST Zip CD

Dear Customer;

OTZ TELECOMMUNICATIONS Telecom regrets that there was a failure in the application of our marketing opt-out mechanism(s). As a result, your CPNI was

_____.

OTZ TELECOMMUNICATIONS respects the privacy of our customers and our employees do everything possible to protect information that may be found in your account records. We apologize for this failure and have taken steps to assure that it does not recur.

Please accept our sincere apologies. It is our goal to have no additional issues with marketing opt-out decisions made by our customers.

Chief Executive Officer

CPNI

Frequently asked Questions

1. What is CPNI?

CPNI stands for customer proprietary network information that is collected and held by wireline or wireless telecommunications carriers. In practical terms, CPNI includes highly sensitive personal information such as the phone numbers called by a consumer, the frequency, duration and timing of such calls, and any services purchased by the consumer, such as call waiting. CPNI does not include subscriber list information.

2. What are the concerns about call privacy?

Numerous companies, known as “data brokers” operate websites where call detail records and other confidential customer information are offered to anyone willing to pay a fee. These companies claim they can access call detail records or wireless location information, and trace cellular or landline phone calls. These companies do not disclose how they obtain information.

Most of the information is obtained through “pretexting” or “social engineering” using fraudulently methods to obtain CPNI. This is where someone uses personal information from sources other than the telecommunication company to impersonate an authorized customer and gain access to the customer’s account without permission from the telecommunication company or the customer.

3. What is the customer’s rights concerning CPNI?

It is the customer’s right under Federal Law to restrict the use of their CPNI. This includes the type of services purchased, how they are used, and any billing information regarding these services.

4. Does the telecommunications company always need approval to use a customer’s information?

Not always. You may use a customer’s information, without approval, to market enhancements to services the customer already uses. For example, if your customer purchases basic local telephone service you do not need their approval to use the customer information to market voice mail or caller ID services to them. On the other hand, if the customer subscribes to local and long distance, you would need the customer’s approval to use their CPNI to sell them wireless service.

However, if the customer asks you to put her residential telephone number on your company-specific do-not-call list, you must do so, and then you cannot even make the calls to enhance existing services.

5. What duties does the telecommunications company have with CPNI?

Generally, every telecommunications carrier has a duty to protect the confidentiality of proprietary information of their customers.

Specifically, all carriers must obtain a customer's knowing consent before using or disclosing CPNI. If a carrier plans to disclose CPNI to third parties or affiliates that do not provide communications-related services, they must obtain affirmative, opt-in consent first.

Section 64.2009 of the FCC's rules has established six "safeguards" for the use of CPNI that apply to all telecommunications companies:

1. Recordkeeping.

You must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI. For example, your software may indicate within the first few lines of the first screen whether or not the customer has given you approval to use his CPNI.

2. Training and Discipline.

You must train your employees as to what CPNI is and when they are and are not authorized to use CPNI. You need to implement a specific disciplinary process to address what happens when an employees fails to follow CPNI rules and procedures.

3. Market Campaigns.

You must maintain a record of your own and any affiliates' sales and marketing campaigns that use your customers' CPNI. All carriers must maintain a record of all instances where it disclosed CPNI or provided CPNI to third parties, or where third parties were allowed access to CPNI. These records must contain a description of each marketing campaign, the specific CPNI that was used in the campaign and what products and services were offered as part of the campaign.

Telecommunication companies must retain these records for a minimum of one (1) year.

4. Supervisory Review Process.

You must require management approval of marketing campaigns that use CPNI and establish a supervisory review process regarding compliance with rules for those marketing campaigns and maintain records of such compliance for a minimum of one (1) year.

5. Compliance Certificates.

This is a two-part requirement. On an annual basis, each telecommunications company must:

- a. *Have an officer sign a compliance certificate stating that the officer has personal knowledge that your company has established operating procedures that are adequate to ensure compliance with the rules.*
- b. *Provide a statement accompanying the certificate explaining how your operating procedures ensure that you are in compliance with the rules.*

You must make the annual compliance certificate and the accompanying statement available for public inspection.

6. *Notice to FCC When Opt-Out Mechanisms Don't Work Properly.*

If you discover or determine that your opt-out mechanisms do not work properly, to "such a degree that a consumer's inability to opt-out is more than an anomaly" you must notify the FCC by written letter within five business days. The letter needs to include your Telecommunication Company name, a description of your opt-out mechanism, the problem(s) experienced, the remedy proposed, and when it will be or was implemented, whether you have notified the FBI and USSS and whether it has taken any action, a copy of the notice you sent to your customers, and your contact information.

6. **What needs to be contained in the "compliance certificate" and the "accompanying statement" required by FCC rule 64.2009(e)?**

The compliance certificate must be signed by an officer, as an agent of the telecommunications company on an annual basis. The compliance certificate must state that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the CPNI rules.

In addition to the brief compliance statement, each company must also prepare a "statement accompanying the certificate" explaining how your operating procedures ensure that you are in compliance with the rules. This statement explains to the FCC how your company complies with the CPNI rules. Information you should maintain in connection with your accompanying statement might include:

- *The type and frequency of employee training on CPNI including any records that were kept about the training, and whether the training was formal or verbal)*
- *The types or instructional or written materials given to employees.*
- *A description of the supervisory process that comes to bear and the consequences that exist if an employee uses CPNI against company policy.*
- *Any personnel manual provisions that address confidentiality of customer information.*
- *How you instruct new employees about the need to keep CPNI confidential.*

7. **What about the letters the FCC Enforcement Bureau recently sent to numerous telco nationwide seeking Compliance Certified for the past five years?**

Some telecommunication companies have received a letter or fax from the FCC Enforcement Bureau stating: "The FCC has initiated an inquiry to determine whether your company has failed to prepare and maintain an adequate CPNI compliance certificate." The letter requests that you provide your compliance certificates and accompanying statements for the past five (5) years.

The FCC letter also requests the telecommunication company provide a supporting affidavit or declaration under penalty of perjury, signed and dated by an officer of the company, with personal knowledge of the representations provided in your response verifying the truth and accuracy of the information.

Some telcos may not have completed a Compliance Certificate or an Accompanying Statement for some prior years. Harsh fines can result from any attempts to "backdate" compliance certificates.

Any telecommunications company who receives this type of a letter from the FCC should seek help. Please call GVNW and request a copy of your prior filings and seek legal counsel for advice on how to proceed.

8. What types of marketing can a carrier conduct without using a customer's CPNI?

General marketing or promotions sent to your entire customer base are not considered to use CPNI. Whenever you send a marketing piece to all of your customers, you have not used CPNI. You make market enhancements to services the customer already uses.

In addition, the FCC rules allow you to conduct a marketing campaign using the following types of generally available information without giving rise to the CPNI rules:

- *General customer information including the customer's name, address and phone number.*
- *Aggregate information where the individual customer identities and characteristics have been removed or are not identifiable.*
- *Information available from directories.*
- *Publicly available information (for example, targeting customers by zip codes or neighborhoods)*

It is only when you use targeted marketing, or customer-specific marketing, that the CPNI rules apply. For example, if you send a special marketing campaign letter only to those customers that use your broadband, then most likely, you used CPNI to determine which customers were on that list.

9. If a telecommunications company plans to use CPNI, what do we need to do?

Before you make any solicitation for customer approval to use CPNI, a telecommunication company must first provide a notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI. The FCC says the notice should have

“enough information to enable the customer to make an informed decision as to whether to permit a telecommunication company to use, disclose, or permit access to the customer’s CPNI.”

To meet this standard, the FCC requires several important features to be included in this notice. Some of these are:

- *State that the customer has a right and the telecommunication company has a duty under federal law to protect the confidentiality of CPNI.*
- *Explain what CPNI is, identify the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customers of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.*
- *Clearly identify the steps a customer must take to grant or deny access to CPNI, and clearly state that a denial will not affect the provision of any services to which the customer subscribes.*
- *State that any approval or denial of approval for the use of CPNI is valid until the customer affirmatively revokes or limits such approval or denial.*
- *The notice must be easily understood, not misleading, clearly legible.*

You must give this notice in close timeframe to any solicitation for customer approval. (One way to accomplish this is to send the notice along with the solicitation for approval). You must maintain records of notification (whether oral, written or electronic) for at least one year”

1. *“Opt-Out” – You may send your customers a notice saying you will consider the customer to have given approval to use his customer information for marketing unless he tells you not to do so. You must wait at least 30 days after giving the notice before you may assume the customer has given approval to use, disclose or permit access to CPNI. If you provide the notifications by mail, the 30-day clock begins three days following mailing date. Telecommunication companies using the opt-out provision must provide notices to their customers every two years.*
2. *“Opt-In” – Telecommunication companies may send customers a notice asking for express permission to the customer information for marketing. You must keep the response on file for at least one (1) year.*
3. *“One-Time Use” of CPNI – Telecommunication companies may use oral notice to obtain a limited, one-time use of CPNI for in-bound or out-bound customer telephone contacts for the duration of that call. That notice must include all the disclosures listed in the first part of this answer, except that you need not remind the customers the following:*
 - a. *The fact that if the customer has opted out previously, then no action is needed to maintain the opt-out election;*
 - b. *If you do not plan to share or disclose the limited information which you are gathering to your affiliates or to third parties, then you need not tell the customer that you might do so.*
 - c. *You need not disclose the means by which a customer can deny or withdraw future access to CPNI so long as you explain that the scope of this request is limited to one-time use.*

- d. *So long as you clearly communicate that the customer can deny access to his or her CPNI during this call, you need not disclose the precise steps the customer must take in order to grant or deny access to CPNI.*

10. Can a telecommunications company use e-mail for the Opt-In or Opt-Out Notices?

Telecommunication companies must obtain express, verifiable prior approval from customers to send notices via email regarding CPNI. If you do so, you must allow customers to respond via email.

11. If a customer gives consent to use their CPNI, what can the telecommunication company, do with that information?

With consent a telecommunication company is able to share CPNI with affiliates, agents and parent companies. Sharing the information enables the telecommunication company to collaborate on how to better serve the customer's telecommunications needs.

12. Can the customer change their mind about giving consent?

A customer has the right at any time to withdraw previously given permission to share CPNI by notifying the telecommunication company.

13. Will the customer be affected in any way if they decide not to provide consent?

The customer decision to disallow the sharing of CPNI will not affect the services that they receive from the telecommunication company.

14. Can a telecommunications company use website notification?

NO. Although your notices can be oral, written or electronic, it must be directed to each specific customer.

15. What if a customer has more than one phone number – Does a Telecommunications company send one letter to each working number, or one to each distinct customer?

You are required to notify each "customer or entity." If a customer or a business has multiple lines, just one notice is enough.

16. If the telecommunications company obtains a customer's consent to use CPNI, can the company disclose the information to others?

If you obtain a customer's "Opt-out" or "Opt-in" approval, you may then disclose that customer information, for the purposed of marketing communications-related services, to your agents, affiliates, joint venture partners and independent contractors that provide communications-related services. You must also enter into agreements with those third parties to make sure they keep the customer information confidential. Any other release of CPNI must have specific "opt-in" approval.

17. What if the customer requests to see their own CPNI or requests our company to supply that information to a third party?

If the customer makes an affirmative written request to disclose that information to a third party, the carrier must honor that request. 47 USC 222(s) (2)

18. What can customers do to protect themselves?

Establishing and using passwords is an action that customers can take to protect themselves.

19. When do the CPNI rules become effective?

A firm effective date has yet to be established for the FCC's new CPNI rules, companies should be ready for an effective date as early as December 8, 2007. The new rules will become effective on December 8, 2007, or on approval by the Office of Management and Budget (OMB), whichever is later.

20. Where do I go for more information?

<http://www.fcc.gov/eb/CPNI/> or <http://www.fcc.gov/cbg/consumerfacts/phoneaboutyou.html>

Or call or e-mail me at: Dorrene Benthin 503-612-4416 dbenthin@gvnw.com

FCC Consumer Advisory

Protecting the Privacy of Your Telephone Calling Records

What Information Does Your Telephone Company Collect?

Your local, long distance and wireless telephone companies collect information such as the numbers you call and when you call them, as well as the particular services you use, such as call forwarding or voice mail. Telephone companies collect this customer information, sometimes called Customer Proprietary Network Information (CPNI), so they can provide the services you have requested and send you bills for them.

Both Congress and the FCC impose requirements on telephone companies about how they can use this information and what they must do to protect it from disclosure. Despite these rules, using a practice known as “pretexting,” or posing as someone such as the actual customer or a law enforcement official, unscrupulous individuals have been able to obtain telephone calling records, and, in some cases, offer them for sale on the Internet. To help control this practice, Congress recently passed a law making it a crime punishable by fine or imprisonment of up to 10 years to obtain calling records from a telephone company, including Voice over Internet Protocol (VoIP) service providers, by: making false or fraudulent statements, providing fraudulent documents, or accessing customer records without prior authorization through the Internet or fraudulent computer-related activities. The law also prohibits the unauthorized sale or transfer of confidential phone records or the purchase or receipt of such information with knowledge that it was obtained fraudulently or without authorization.

What Can Your Telephone Company Do With This Information?

Both a law passed by Congress and Federal Communications Commission rules impose a general duty on telephone companies to protect the confidentiality of your customer information. Telephone companies may use, disclose, or permit access to your customer information in these circumstances: (1) as required by law; (2) with your approval; and (3) in providing the service from which the customer information is derived.

Your telephone company must disclose your customer information to any person you designate if you make a request in writing. Your telephone company may use your customer information, without your approval, to market enhancements to services you already use. For example, if you purchase basic local telephone service from a telephone company, it does not need your approval to use your customer information to try to sell you voice mail or caller ID services. However, if you ask your telephone company to put your residential telephone number on its company-specific do-

not-call list, it cannot legally make these calls.

If your telephone company uses your customer information for other marketing, it must obtain your approval to do so. The company may request your approval orally, in writing, or electronically. The request must contain specific disclosures about how your telephone company will use your customer information. The company can request your approval using one of two methods:

1) **“Opt-Out”** – Your telephone company sends you a notice saying it will consider you to have given your approval to use your customer information for marketing **unless you tell it not to do so** (usually within 30 days.)

2) **“Opt-In”** – Your telephone company sends you a notice asking that you **expressly give it permission to use your customer information** for marketing.

Your telephone company must obtain your “opt-out” or “opt-in” approval before it can share your customer information within the company to sell you services you don’t already purchase, i.e., to sell you wireless service if you only subscribe to local and long distance service. If your telephone company obtains your “opt-out” or “opt-in” approval, it may also disclose your customer information, for the purpose of marketing communications-related services, to its agents, affiliates, joint venture partners and independent contractors that provide communications-related services. To disclose your customer information to agents, affiliates, joint venture partners, or independent contractors that do not provide communications-related services, or to any other third parties, your telephone company must obtain your “opt-in” approval. If your telephone company discloses your customer information to joint venture partners or independent contractors, it must enter into agreements with them to keep your customer information confidential.

What Must Your Telephone Company Do To Keep Your Information Confidential?

The FCC requires your telephone company to keep accurate records of all instances where your customer information was disclosed or provided to third parties, and whether or not you have provided approval to use your customer information for marketing. Telephone companies must train their employees in the appropriate use of customer information. Marketing campaigns using customer information must be carefully reviewed. The FCC requires telephone companies to prepare annual compliance certificates signed by an officer of the company certifying that the company has established operating procedures that are adequate to ensure compliance with these rules. The compliance certificates must be made publicly available.

What Is The FCC Doing To Keep Your Telephone Company From Disclosing Your Information?

In addition to these rules, the FCC is exploring whether new or stronger rules may be necessary to protect your customer information. The FCC investigates consumer complaints about unauthorized

or unlawful disclosure of customer information, and, if it finds a violation, can issue citations and propose fines. The FCC recently proposed \$100,000 fines on telephone companies with inadequate certifications regarding compliance with FCC rules protecting customer information from disclosure.

The FCC also works closely with the Federal Trade Commission (FTC) to prevent the unlawful sale or distribution of customer information by data brokers or Web sites. Telephone companies also have sued data brokers to prevent the unlawful sale or distribution of customer information.

You are an important part of the FCC's efforts to keep telephone companies from unlawfully disclosing your customer information. If you suspect that your customer information may have been disclosed without your permission, first contact your telephone company to inform it of your concern. If you don't think your customer information is being protected adequately, file an informal complaint to help the FCC determine if there is a problem. You can file a complaint with the FCC by e-mail (fccinfo@fcc.gov), the Internet (<http://www.fcc.gov/cgb/complaints.html>), telephone 1-888-CALL-FCC (1-888-225-5322) voice or 1-888-TELL-FCC (1-888-835-5322) TTY, fax (1-866-418-0232), or mail.

If mailing a complaint, send it to:

Federal Communications Commission
Consumer & Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
445 12th Street, SW
Washington, DC 20554.

How Can I Help Prevent Unauthorized Disclosure of My Information?

- If you think your customer information has been disclosed without your permission, contact your telephone company right away. Also, file a complaint with the FCC.
- Ask your telephone company to provide information about what it does to protect the confidentiality of your customer information.
- Read your telephone bill and any other notices you receive from your telephone company carefully. Determine if your telephone company is seeking opt-in or opt-out permission to use or share your customer information for marketing.
- Make your choice about sharing your customer information clear to your telephone company. The choice you make about how your customer information is used and shared is valid until you inform your telephone company that your choice has changed.
- If you use a password when contacting your telephone company to obtain your customer information, avoid using any sensitive or readily apparent information, such as your social security number.

Remember: Customer information rules apply to all telephone companies: local, long distance, and

wireless. Make your customer information choices known to each company.

For more information on telephone company issues, visit www.fcc.gov/cgb; ; send an e-mail to fccinfo@fcc.gov; or call us at 1-888-CALL-FCC (1-888-225-5322) (voice) and 1-888-TELL-FCC (1-888-835-5322) (TTY).

For this or any other consumer publication in an accessible format (electronic ASCII text, Braille, large print, or audio) please write or call us at the address or phone number below, or send an e-mail to FCC504@fcc.gov.

To receive information on this and other FCC consumer topics through the Commission's electronic subscriber service, click on <http://www.fcc.gov/cgb/contacts/>.

This document is for consumer education purposes only and is not intended to affect any proceeding or cases involving this subject matter or related issues.

01/18/07

Federal Communications Commission • Consumer & Governmental Affairs Bureau • 445 12th St.
S.W. • Washington, DC 20554



1-888-CALL-FCC (1-888-225-5322) • TTY: 1-888-TELL-FCC (1-888-835-5322) • Fax: 1-866-418-0232
• www.fcc.gov/cgb/